UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,526	08/16/2001	Arindam Das-Purkayastha	B-4274 618998-3	3735

22879 7590 08/15/2006

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,526	DAS-PURKAYASTHA ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Original application contained claims 1 – 6 filed on 8/16/2001. New claims 7 – 61 have been added in an amendment filed on 12/24/2004. Presently, pending claims are 1 – 61.

Response to Arguments

2. In view of the remarks filed 7/10/2006, the 35 U.S.C. 101 rejections on claims 1, 6, 7, 24 and 42 and the claim objection on claim 42 have been withdrawn.

3. ***For purpose of appeal***, PROSECUTION IS HEREBY REOPENED to maintain a clean record and clarity of 35 USC § 102 rejections to avoid unnecessary confusion when presenting to the board.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 – 9, 11 – 19, 24 – 26, 28 – 37, 40, 42 – 55 and 58 are rejected under 35 U.S.C. 102(e) as being anticipated by Grawrock (U.S. Patent 6,678,833).

As per claim 1 and 6, Grawrock teaches a computer apparatus, comprising:

a receiver for receiving an integrity metric for a computer entity via a trusted device (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger) **associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity** (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15).

a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric (Grawrock: Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6: TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level).

As per claim 7, Grawrock teaches a method for establishing communications with a computer entity, comprising:

requesting a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity; receiving a response from the trusted device including an integrity metric calculated for the entity by the trusted device (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger);

comparing values in the integrity metric (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15) **calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party** (Grawrock: Column 4 Line 9 and Column 4 Line 35 – 37: the challenger that verifies and determines the trust level (i.e. trusted or un-trusted) is interpreted as the trusted party that must provide the authentication values for comparing against the integrity metrics reported by the TPM so that whether the platform is trusted or not can be determined accordingly, as taught by Grawrock); and

selecting a level of trust for the entity from a plurality of predefined levels of trusts based on at least one value in the integrity metric calculated for the entity by the trusted device (Grawrock: Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6: TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level).

As per claim 24, Grawrock teaches a method for a computer entity to respond to a request for integrity check prior to exchanging data, comprising:

receiving at a trusted device associated with a computer entity a request to provide an integrity metric containing values indicative of one or more characteristics of the entity (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger);

calculating at the trusted device values indicative of one or more characteristics of the entity (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the

disclosure of the instant application (SPEC: Page 11 Line 10 – 15); and providing a response from the trusted device including an integrity metric including the values indicative of one or more characteristics of the entity (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6).

As per claim 42, Grawrock teaches a method for establishing communications between a computer entity and a user, comprising:

presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device; presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: the challenger is considered as the user, and TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger) and containing values indicative of one or more characteristics of the entity (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15);

comparing at the user (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can

accurately report the integrity metric upon the request issued by the challenger so that the challenger can determine that the platform has been properly initialized and is trusted) values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party (Grawrock: Column 4 Line 9 and Column 4 Line 35 – 37: the challenger that verifies and determines the trust level (i.e. trusted or un-trusted) is interpreted as the trusted party that must provide the authentication values for comparing against the integrity metrics reported by the TPM so that whether the platform is trusted or not can be determined accordingly, as taught by Grawrock); and

selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device (Grawrock: Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6: TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level).

As per claim 2, Grawrock teaches the trusted device is arranged to acquire an integrity metric of the computer entity (Grawrock: Column 3 Line 62 – Column 4 Line 9).

As per claim 3, Grawrock teaches the trust level is determined by comparing the value of the at least one characteristics with a specified value (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6).

As per claim 4, Grawrock teaches the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6).

As per claim 5, Grawrock teaches the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics for a plurality of computer entities (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6).

As per claim 8, 11, 25, 28, 43 and 46, Grawrock teaches the trusted device is hardwired to the computer entity (Grawrock: Column 4 Line 21 – 23).

As per claim 9, 26 and 44, Grawrock teaches the trusted device is configured to control the boot process of the computer entity (Grawrock: Column 3 Line 61 – 67).

As per claim 12, 29 and 47, Grawrock teaches the trusted device is configured to contain one or more of a public encryption key, a private encryption key (Grawrock:

Column 4 Line 13 – 19: the TPM must contain the public / private key-pair; otherwise, the requested / response information can not be decrypted / encrypted properly), and one or more authenticated values provided for the entity integrity metric by the trusted party (Grawrock: Column 4 Line 9 and Column 4 Line 10 – 11: (a) the challenger verifies the results and determines the trust level and as such the challenger must contain the respective authenticated values (b) the challenger can be an internal device within the TPM, as taught by Grawrock, and therefore authenticated values must be also within the TPM (i.e. challenger)).

As per claim 13, 30 and 48, Grawrock teaches the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity (Grawrock: Column 3 Line 61 – 67 and Column 4 Line 7 – 9).

As per claim 14, 31 and 49, Grawrock teaches the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity (Grawrock: Column 4 Line 1 – 9: the boot block identifiers can be considered as part of the system configuration information to trace different version# of BIOS code).

As per claim 15, 32, 36, 50 and 54, Grawrock teaches the components of the entity are selected from among the group of components comprising hardware components and software components (Grawrock: Column 4 Line 1 – 6).

As per claim 16, 33 and 51, Grawrock teaches wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM, operating system loader, and operating system of the entity (Grawrock: Column 4 Line 3 – 6).

As per claim 17, 34 and 52, Grawrock teaches the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information (Grawrock: Column 4 Line 15 – 18: for example, certificate).

As per claim 18, 35 and 53, Grawrock teaches the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components (Grawrock: Column 4 Line 1 – 9).

As per claim 19, 37 and 55, Grawrock teaches the response received from the trusted device includes the authenticated values provided by the trusted party (Grawrock: Column 4 Line 35 – 40).

As per claim 40 and 58, Grawrock teaches the request includes input data (Grawrock: Column 4 Line 13 – 16).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 10, 27 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (U.S. Patent 6,678,833), in view of Saunders (U.S. Patent 6,209,099).

As per claim 10, 27 and 45, Grawrock does not disclose expressly the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

Saunders teaches the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device (Saunders: Figure 3 Element 28: no further response from the trusted device if the boot key is not entered and configured).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Saunders within the system of Grawrock because (a) Grawrock teaches protecting information and accurately reporting this information by using a trustworthy TPM (Trusted Platform Module) (Grawrock : Column 1 Line 65 – 67) and (b) Saunders teaches providing a mechanism to decide whether the components of the system (including both hardware and software

components) are really trustworthy without modification (Saunders: Column 1 Line 11 – 17).

6. Claims 20, 21, 38, 39, 41, 56, 57 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (U.S. Patent 6,678,833), and in view of Stoltz (U.S. Patent 6,615,264).

As per claim 20, 38 and 56, Grawrock does not disclose expressly generating a nonce to pass to the trusted device with the request.

Stoltz teaches generating a nonce to pass to the trusted device with the request (Stoltz: Column 17 Line 64 – 66, Column 18 Line 1 – 5: nonce is a random number).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Stoltz within the system of Grawrock because (a) Grawrock teaches protecting information and accurately reporting this information by using a trustworthy TPM (Trusted Platform Module) with the request initiated from an external device (Grawrock : Column 1 Line 65 – 67 and Column 4 Line 12) and (b) Stoltz teaches a security enhanced method to authenticate the request for secure information in a client-server networking system – i.e. from an external device respective to the TPM system (Stoltz: Column 3 Line 65 – Column 4 Line 2, Column 4 Line 9 – 12, Column 17 Line 64 – 66 and Column 18 Line 1 – 5).

As per claim 21, 39 and 57, Grawrock as modified further teaches the response from the trusted device includes the nonce received with the request (Stoltz: Column 18 Line 46 – 47).

As per claim 41 and 59, Grawrock as modified teaches the response includes the input data processed with the private encryption key (Stoltz: Column 18 Line 41 – 43: the response includes the encryption of the random number, which is part of the input information during the request). See the same rationale address above in rejection claim 20.

7. Claims 22 – 23 and 60 – 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (U.S. Patent 6,678,833).

As per claim 22 and 60, Grawrock teaches the requester (or challenger – an external device) verifies and determines the trust level (i.e. trusted or un-trusted) of the respective computer entity with which it attempts for establishing communications Grawrock: Column 4 Line 9, Column 4 Line 35 – 37 and Column 4 Line 12: challenger is an external device). Grawrock does not disclose expressly initiating data transfer to the entity in accordance with the selected trust level.

Howeve, It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Grawrock to accommodate initiating data transfer to the entity in accordance with the selected trust level because a person of

ordinary skill would recognize the risk and avoid transferring data with an unsecured system once the trusted level (i.e. either trusted or un-trusted) of the target computer entity has been evaluated by the user / challenger / external device, as taught by Grawrock (Grawrock: Column 4 Line 35 – 37).

As per claim 23 and 61, Grawrock as modified further teaches initiating data transfer to the entity in accordance with the selected trust level comprises transferring no data (See the same rationale as set forth in rejecting claim 22).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100